Secure Electronic Healthcare Record Using Robust Authentication Scheme

Aqeel A. Yaseen, Kalyani Patel, Ali A. Yassin, Abdulla J. Aldarwish, Haitham A. Hussein

***Abstract*— Electronic Healthcare Record (EHR) has been actively promoted recently. Healthcare records and paper-based medical prescriptions are scattered and unorganized in medical institutions and clinics, thereby prompting many efforts to advance the EHR from traditional clinical settings to an efficient electronic medical model to regulate health records appropriately and accurately. With the development of technology and data exchange over the Internet or local networks, protecting transmitted data in healthcare records is necessary. This paper presents a secure EHR system utilizing robust authentication and RSA digital signature. We performed formal and informal security analyses utilizing the Scyther tool and the Canetti–Krawczyk (CK) model. Therefore, the proposed scheme has a higher level of security than the previous relevant work by resisting the dangers of well-known cyberattacks, such as impersonation, DoS, replay, man-in-the-middle (MITM), and insider attacks. Our work balances the security complexity and the communication cost, and the comparison tables show that the proposed scheme has the lowest communication cost. Moreover, we presented a secure prescription through a QR code generated using the prescription and the physician's RSA digital signature.**

***Index Terms*—Keywords: Healthcare System, Authentication, Secure Prescription, RSA Signature, QR code**

I. INTRODUCTION

SINCE the digital mutation in many fields and the revolution of information technology, the transition from paper to electronic healthcare record (EHR) has become urgent and necessary. Healthcare institutions strive to collect a vast number of patients' medical information. Moreover, the unorganized notes of hospitals, clinics, laboratories, and other health institutions concerning patients' cases and their sensitive data lead to arbitrary management. This condition is also time-consuming for physicians when reviewing a patient's case. EHR is considered a perfect solution to organize medical information [1-3].

Manuscript received Aug. 13, 2022; revised Mar 27, 2023.

Aqeel A. Yaseen is a PhD candidate of Department of Computer Science, Gujarat University, Ahmedabad, 380009, India (e-mail: aay.ali80@gmail.com).

Kalyani Patel is an Assistant Professor at K.S. School of business Management and Information Technology, Gujarat University, Ahmedabad, 380009, India (e-mail: kalyanipatel@gujaratuniversity.ac.in)

Ali A. Yassin is a Professor of Computer Science Department, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq (e-mail: ali.yassin@uobasrah.edu.iq).

Abdulla J. Aldarwish is a Lecturer of Computer Science Department, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq (e-mail: abdullajas@uobasrah.edu.iq).

Haitham A. Hussein is a Lecturer of Accounting Technologies Department, Southern Technical University, Basrah, 61001, Iraq (e-mail: haitham.ali@stu.edu.iq).

EHR entities, such as patients, physicians, and pharmacies, share the medical information of patients, and EHR environment is portioned into a collaborative partner (hospital and physician), the entities which exchange data, and the requester (clinical laboratories, pharmacists, and physicians). At the same time, the data users are the patients and their families or friends [1, 4, 5]. EHR must ensure access and data sharing securely. Fig. 1 shows the data exchange securely utilizing authentication among different EHR entities.

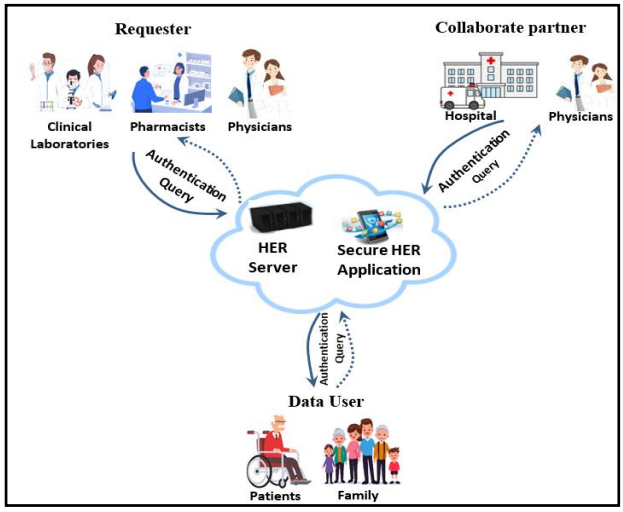

Fig. 1 Secure Connections among EHR Entities

Many secure and trusted techniques have been proposed recently in accordance with the sensitivity of healthcare data and the exchange of information via healthcare systems and applications. The integration and reinforcement of such security techniques improve the accuracy and quality of EHR systems. Accordingly, EHR systems/ applications are built with a high level of caution and precision for secure registration and login to the system, whether for the patient, the doctor, or any other system entities. However, unauthorized individuals (intruders/attackers) seize appropriate opportunities to find a system vulnerable to attack [5, 6]. Thus, login authentication is considered the backbone of any security design to prevent unauthorized individuals or robots using passwords, biometrics, and tokens. Regardless, the authentication type, the use of authentication is very important for each security system. Initially, a password or smart card PIN operates one factor, commonly known as single-factor authentication (SFA), which is the simplest type of authentication used to confirm the user's identity. Sharing

the password itself makes the account vulnerable. In addition, an unauthorized user may attempt to acquire access using social engineering methods, the rainbow table, or dictionary attacks [7-9]. Two-factor authentication (2FA) is adopted as an enhancement and reinforcement that combines the user name and password with a factor of personal ownership, such as a smartcard or a phone [10]. Then, and a step forward, multi-factor authentication (MFA) was suggested to provide a greater level of security and continuously secure computer equipment and other essential services from illegal access by utilizing more than two factors [8, 11]. Currently, three crucial sorts of MFA are available, as follows:

- Something the individuals know (e.g., password, PIN, or KBAs).
- Something the individuals have (e.g., smart phone, debit card, or any other smart card)
- Something the individuals are, literally a unique identifier biometric (e.g., fingerprint, speech patterns, or facial structure)

Existing applications are implemented to balance convenience and security by utilizing multiple authentications, which could be the best case for modern MFA [8, 10-12].

The proposed scheme presents a secure EHR model and modern facilities (e.g., QR) that can facilitate work between the system entities. The proposed scheme of EHR entities distinguishes the distribution of permissions and privileges as a contribution to our research. The authentication of information is exchanged among EHR system entities, data integrity, entity verification as mutual authentication, and digital signature. These security techniques were considered in the proposed work scheme, as follows:

1. Secure registration for doctors and patients by specifying an anonymous health center (AHC). AHC is responsible for the registration and distribution of secret keys, as well as the permissions and privileges granted.
2. MFA upon EHR system login. The proposed scheme preserves the system entities' privacy and resists malicious attacks, such as man-in-the-middle (MITM), insider attacks, and reply attacks. In addition, mutual authentication uses the RSA signature between the doctor and hospital healthcare server (HHS) to verify each other. Moreover, a biometric has been employed with the MFA to increase the immunity of the proposed scheme.
3. The doctor must prepare a prescription treatment. It is provided securely and exchanged safely among the system entities to prevent harm by intruders. It must be signed by the doctor through RSA signature and sent to the specified entity (e.g., pharmacist).
4. Security analysis has been conducted using informal and formal tools (Scyther Verification Tool) to improve the sobriety of the proposed scheme.

The remainder of the paper is organized as per follows: Section 2 reviews the related work. Section 3 presents the proposed healthcare secure schemes and justified by security analysis in Section 4. Finally, Section 5 presents the conclusion.

II. Related work

The privacy of user data is ensured by preventing sensitive information from being harmed by intruders and unauthorized persons. Such security challenges currently receive increased attention from researchers and specialists, and appropriate solutions are developed to protect users' privacy and data from threats posed by malicious attacks. Consequently, EHR and their diverse data demand the highest level of security [1, 6]. In this regard, numerous approaches and studies were presented, including classical techniques, such as steganography and cryptography [13]. At the same time, the requirements of the developing environment for health care records cannot be satisfied by the traditional methods outlined. As an inference, some modern features and techniques have been combined to extend the conventional mechanisms to satisfy the EHR requirements and ensure easy usage and flexibility in handling the EHR [1, 6, 13]. Some examples of extended techniques are multi-factor authentication (MFA), role-based access control (RBAC), digital signatures, and QR code.

Authentication is confirmed as a vital technique for modern security aspects. Some presented schemes enjoyed robust authentication. Even though Saeed Ullah Jan et al. [14] presented a scheme of certificateless signatures for wireless body area networks that maintain the same signature size and is lightweight and secure, security and performance must be balanced. In addition, Jayabalan et al. [15] proposed a robust model utilizing blockchain technology to protect healthcare data administration. However, the computation time cost according to symmetric cryptography (AES-128) must be considered to achieve compatibility among security, cost, and performance.

B. Maciej et al. [16] presented MFA with one-time passwords (OTP), and biometric approaches are often recommended in mobile applications because MFA is more common in mobile and smart contexts, according to mentioned studies. Similarly, T. Abayomi–Zannu et al. [17] worked with blockchain-based e-voting on mobile devices using VIN, PIN, and OTP.

Wahsheh and Al-Zahrani [18] utilized QR codes to scan the healthcare information instead of memorizing these data using a smartphone or any other preferred device. In context, Fauzi et al. [19] utilized QR codes in secure data for the admin or authorized persons to provide a door lock system. QR technology and Raspberry Pi processor were used to access doors securely.

Numerous studies on biometrics were presented in different fields. Lui et al. [20] introduced a scheme for wireless body area networks (WABN), healthcare, and authentication by integrating biometrics with a password and using it with the symmetric encryption key. In addition, A. Alhayajneh et al. [21] presented a sufficiently suitable physiological-based scheme depending on the patients' bodily features for authentication dedicated to WABN. However, the major weakness is that it does not resist DoS attacks, and assessing identical physiological signals for all devices placed on different sections of a patient's body is challenging. In summary, this study contributes to (1) designing a secure MFA that enjoys flexibility and scalability for patient usage, (2) providing a secure communication channel through an AHC, (3) distributing privileges and

permissions among system entities to distinguish the registration phase and the distribution of keys (shared key, secret key, and public key), (4) conducting formal and informal security analyses to verify the proposed scheme's high-level security and resistance to the well-known malicious attacks. Eventually, the presented scheme addressed the problems in the previous related works.

III. Our Proposed Work

In this section, we propose a secure healthcare system that depends on three main elements: requesters (doctors and pharmacist), collaborators (doctors and hospitals), and data users (patients and family). We focus on the authentication side of the two entities (requester: physicians and data user: patients). Moreover, the proposed authentication scheme consists of four phases: registration, login and authentication, secure exchange data, and data integrity. Table I shows the definition of the parameters used in the presented scheme.

TABLE I
Definition of Parameters Used.

Symbol	Description
EHR	Electronic Healthcare Record
$FName_{P_i}$	Patient's full name
Add_{P_i}	Patient's address
P_i	Patient in the system.
Dr_i	Physician
HHS	Hospital Healthcare Server
Un_{P_i}	Patient's username
PW_{P_i}	Patient's password
Un'_{P_i}	Hashed patient's username
PW'_{P_i}	Hashed Patient's password
SK_{P_i}	Shared key generated by AHC
$FName_{Dr_i}$	Physician's full name
Add_{Dr_i}	Physician's address
Un_{Dr_i}	Physician's username
AHC	Anonymous Health Center (Trusted Third Party)
PW_{Dr_i}	Physician's password
PW'_{Dr_i}	Hashed (PW_{Dr_i})
Un'_{Dr_i}	Hashed (Un_{Dr_i})
RSA	RSA signature
FX_{Dr_i}	File of biometric features
B_{Dr_i}	Biometric
$\{n, e\}$	Public key in RSA signature
$\{n, d\}c$	Private key in RSA signature
R	Request of system entities
$\oplus$	Exclusive or
$\|\|$	Concatenation
r_{Dr_i}	Doctor's random no.
h_{Dr_i},	Hashed (r_{Dr_i})
s_{Dr_i}	Doctor's signature

Table II lists the primitive tools used to reinforce our proposed scheme.

TABLE II:
Primitive Tool Description

Tool	Description	Using
Hash Function	SHA-256	System phases
RSA	RSA Digital signature	Doctor Login phase
Scyther	Security Tool Analysis	Formal Security analysis
CK	Canetti–Krawczyk Security Tool Analysis	Informal security analysis

A. Registration phase

This section is divided into two folds as follows:

1. Patient Registration

The patient wishes to register his personal information (Full name ($FName_{P_i}$), Address (Add_{P_i}), Username (Un_{P_i}), and Password (PW_{P_i})) in the healthcare system via the HHS using an AHC to generate keys between entities. Then, this information is crucial for creating the patient's EHR (EHR_{P_i}). HHS verifies the availability of the patient in his database if the existing registration request is canceled; otherwise, HHS computes the anonymous identity of the patient based on the crypto-hash (SHA-256) function as follows:

$Un'_{P_i} = h(Un_{P_i})$

$PW'_{P_i} = h(PW_{P_i} || Un_{P_i})$

Subsequently, HHS sends the request (R) to AHC to generate a shared key SK_{P_i} to perform secure exchange of information in the next phases. The patient registration dialogue is as follows:

$P_i \rightarrow HHS: R = \{Req, FName_{P_i}, Add_{P_i}, Un_{p_i}, PW_{P_i}\}$

$HHS \rightarrow AHC: R = \{Req, Un'_{P_i}, PW'_{P_i}\}$

$AHC \rightarrow HHS: R = \{SK_i\}$

$HHS\ P_i: R = \{SK_i\}$

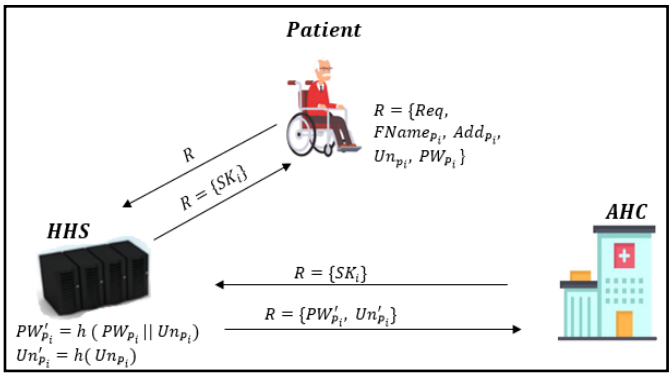

Fig. 2. Patient Registration Phase

2. Doctor registration

The doctor should register his personal information (Full name ($FName_{Dr_i}$), Address (Add_{Dr_i}), Username (Un_{Dr_i}), Biometric (B_{Dr_i}), and Password (PW_{Dr_i})) in the healthcare system via the HHS using an AHC to generate public/private keys using RSA signature between entities. The doctor can apply many operations on EHR_{P_i}, such as read, add, write, and update. The HHS verifies the availability of the doctor in his database if the existing registration request is canceled; otherwise, HHS computes the anonymous identity of the doctor based on the crypto-hash function as follows:

$FX_{Dr_i} = FEXBio(B_{Dr_i})$

$Un'_{Dr_i} = h\,(\,Un_{Dr_i} || \,FX_{Dr_i})$
$PW'_{Dr_i} = h\,(\,PW_{Dr_i} || \,FX_{Dr_i})$
where $FEXBio$ represents the feature extraction function, which responds to save the feature extraction of a doctor's biometric inside the file FX_{Dr_i} saved in an external device, such as a mobile phone or memory stick. Subsequently, HHS sends the request (R) to AHC to generate the Public {n, e} /Private {n, d} key to perform exchange of information in the next phases securely. The doctor's registration dialogue is as follows:
$Dr_i \rightarrow HHS$: $R = \{Req, FName_{Dr_i}, Add_{Dr_i}, Un_{Dr_i}, B_{Dr_i}\}$
$HHS \rightarrow AHC$: $R = \{Req, Un'_{Dr_i}, PW'_{Dr_i}, B_{Dr_i}\}$
$AHC \rightarrow HHS$ $R =$
$\{\, public\ key\{\boldsymbol{n}, \boldsymbol{e}\}, private\ key\{\boldsymbol{n}, \boldsymbol{d}\}, FX_{Dr_i}\}$
$HHS \rightarrow Dr_i$: $R = \{private\ key\{\boldsymbol{n}, \boldsymbol{d}\}, FX_{Dr_i}\}$

Typically, n and d must be selected as large integers (e.g., 3072 bits), whereas e should be a small value. By definition, the RSA key-pair property is as follows:
$(m^e)^d \equiv (m^d)^e \equiv m\ (mod\ n)$, where the rang of all $m\ in\ [0 \ldots n)$

B. Login and strong authentication phase

In this section, we focus on the permission provided to the doctors and patients to secure login to the system. The current phase is divided into two parts, as follows:

1. Patient side:

P_i should follow the steps below to verify his login request:

- Generate an integer random number $r_i \in Z$,
- Compute $Un'_{P_i} = h(\,Un_{P_i})$ and $PW''_{P_i} = h\,(\,PW_{P_i} || \,Un_{P_i}) \oplus r_i$. We notice the significance of the current step by generating a password for each patient's login request.
- Compute $r'_i = r_i \oplus SK_i$ and send query $\{R_{P_i} = <Un'_{P_i}, PW''_{P_i}, r'_i>\}$ to HHS.
- Upon receipt of the patient's query (R_{P_i}), HHS seeks Un'_{p_i} with his DB; if it does not exist, then the login process is terminated. Otherwise, HHS computes $r''_i = r'_i \oplus SK_i$ and $PW'''_{P_i} = PW'_{P_i} \oplus r''_i$. PW''_{P_i} is compared with PW'''_{P_i}; if the result matches, then the patient is granted the privilege to login the system. Otherwise, access is denied.
- After completing the preceding procedures, the key session between the HHS and the patient is managed by ($r_i \oplus SK_i$). Eventually, the patient may access his EHR

2. Doctor side:

Dr_i can access the system when he does not change his device. This method is called smart factor authentication, indicating that the doctor applied the following steps once for each device:

- Dr_i enters his username (Un_{Dr_i}), FX_{Dr_i}, and password (PW_{Dr_i}). Then, he generates a random integer number $r_{Dr_i} \in Z$ and computes $Un'_{Dr_i} = h(\,Un_{Dr_i} || \,FX_{Dr_i})$, $PW''_{Dr_i} = h\,(\,PW_{Dr_i} || \,FX_{Dr_i}) \oplus r_{Dr_i}$, and $r'_{Dr_i} = r_{Dr_i} \oplus FX_{Dr_i}$, where FX_{Dr_i} is stored in the doctor preferred device.
- Dr_i sends his request $R_{Dr_i} < Un'_{Dr_i}, PW''_{Dr_i}, r'_{Dr_i} >$ to HHS.
- Upon receipt of R_{Dr_i}, the HHS checks Un'_{Dr_i}in DB; if it does not exist, then the current process is terminated. Otherwise, he restores $r''_{Dr_i} = r'_{Dr_i} \oplus FX_{Dr_i}$, and then compares PW''_{Dr_i} with ($PW'_{Dr_i} \oplus r''_{Dr_i}$). If they match, then he computes $h_{Dr_i} = h(r''_{Dr_i})$, signs $s_{Dr_i} = h(r''_{Dr_i})^d\ mod\ n$, and replies $R_{HHS} < h_{Dr_i}, s_{Dr_i} >$ to Dr_i.
- Dr_i verifies $s_{Dr_i}$to ensure the validity of the HHS based on $h'_{Dr_i} = {s_{Dr_i}}^e\ (mod\ n)$. He compares h_{Dr_i} with h'_{Dr_i}. If they match, then the HHS is considered reliable. Otherwise, the doctor discovers that the HHS is an unsecured server.

C. Treatment phase

Usually, the doctors in the healthcare institutions prepare a prescription carefully. Such a prescription should be exchanged between doctors or any other important entity in the system. In a similar context, it is added to the patients' EHR. Therefore, the exchange of prescriptions must be performed securely. In other words, unauthorized individuals, such as intruders or attackers, could intercept the sensitive information contained in a prescription. To protect the accuracy and integrity of prescription information during transmission between entities in the EHR system and to prevent unauthorized parties from modifying the prescriptions, the following steps are necessary for the current phase:

- Dr_i writes the prescription (Pr_{Dr_i}), $h_{Pr_{Dr_i}} = h(Pr_{Dr_i})$, signs $s_{Pr_{Dr_i}} = (\,h_{Pr_{Dr_i}})^d\ mod\ n$
- QR codes are generated including ($Pr_{Dr_i}, s_{Pr_{Dr_i}}$), and $R_{Dr_i} < QR >$ is sent to HHS.
- HHS auto-scans the received QR to extract the contents of the QR, verifies $s_{Pr_{Dr_i}}$ based on $h'_{Pr_{Dr_i}} = {s_{Pr_{Dr_i}}}^e\ (mod\ n)$ to ensure the validity of the prescription, then sends it to the pharmacists. He compares $h(Pr_{Dr_i})$ with $h'_{Pr_{Dr_i}}$. If they match, then he sends it to the pharmacists and updates the EHR of the patient using the added prescription. Otherwise, the prescription is invalid and is not sent to the pharmacists.
- If the pharmacist receives a printed prescription from an outpatient, then it should bear a QR code, including the doctor's signature. Then, the pharmacist scans and makes a copy of the QR code and then sends it to the HHS to ensure the validity of the doctor's signature. Once the validity is confirmed, the pharmacist can dispense the treatment to the patient. Fig. 4 shows the treatment phase steps.

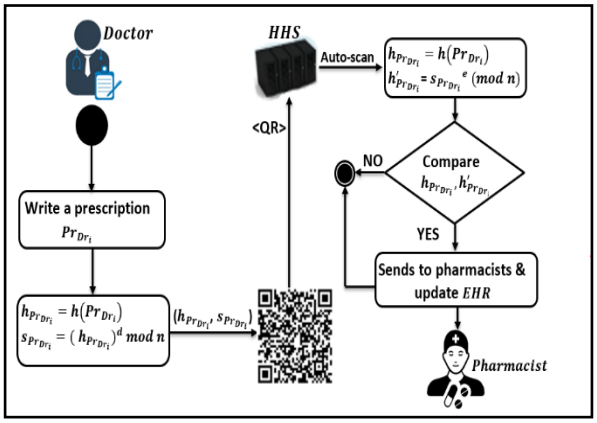

Fig. 4. Treatment phase

IV. Security Analysis

This section examines the security of the proposed protocol using formal and informal security analyses. The formal analysis utilized a tool called Scyther tool.

A. Formal security analyzing

Scyther is a tool for officially analyzing security protocols, their security needs, and potential flaws. It is a new checking and verification model compared with SPIN and PRISM models [22, 23]. The protocol analysis depends on Scyther called informal analysis. The traditional system that does not use the security techniques in the Scyther tool is rejected. Fig. 5 shows the weakness of the conventional system when the proposed protocol is performed without using the security functions.

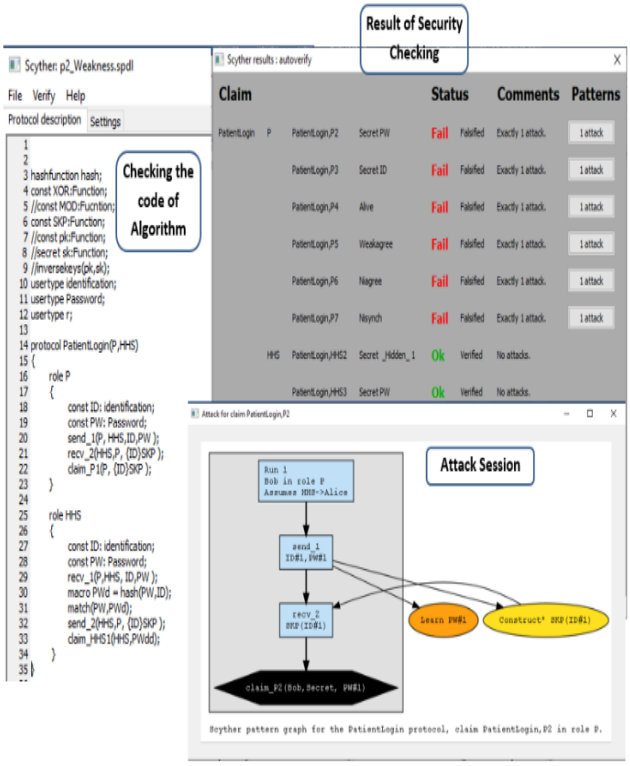

Fig. 5. Weakness of the traditional system

The results in Fig. 6 verify the security of the proposed system. The results clarify that the proposed system is unreachable and is resistant to well-known attacks. This figure represents the algorithmic steps for patient login. Fig. 7 shows the result of the proposed Scyther analysis for doctor login in the EHR system.

B. Informal security analysis

In this section, to prove the security of our proposed scheme, the informal security analysis was conducted using the Canetti–Krawczyk (CK) threat security model [24]. The security challenges could be summarized as follows:

- **Anonymity**: well-known malicious attackers that attempt to expose secret information by detecting any system vulnerability. The anonymity is addressed as follows:
  1. AHC is allocated within a health institution and is responsible for key distribution among the system entities. This step increases the complexity of malicious attacks.
  2. To complicate the intruder's task of exposing system entities' crucial information (username/password), the login information preserved anomaly to the HHS using hash function SHA-256, as follows:

Patient:

$$Un'_{P_i} = h(\,Un_{P_i}),$$
$$PW'_{P_i} = h\,(\,PW_{P_i} \,||\, Un_{P_i})$$

Doctor:

$$Un'_{Dr_i} = h\,(\,Un_{Dr_i} || \,FX_{Dr_i}),$$
$$PW'_{Dr_i} = h\,(\,PW_{Dr_i} \,||\, FX_{Dr_i})$$

- **Session key management:** the session key has been preserved securely. Especially after validating the patient identity during the login phase, the agreement on a session key $r_i \oplus SK_i$ is ensured. The patient information are saved from adversaries using r.
- **Unlinkability:** the proposed scheme prevents the attackers from linking the multiple actions of the doctor/patient, such as a previous login to the system, by changing the values $(SK_i\ , PW_{P_i}, r_i)$ for each login process. Therefore, the patient can login to the system multiple times with unlinkability by the attackers.
- **Mutual Authentication:** a mutual authentication feature was achieved through the doctor's login phase (Dr_i to $HHS \leftrightarrow HHS$ to Dr_i). Through the parameters (r'_{Dr_i}) already sent by the user, the HHS must ensure the validity of the doctor in his DB. Subsequently, $R_{HHS} < h_{Dr_i}, s_{Dr_i} >$, $h(r''_{Dr_i})$, and the RSA signature of $h(r''_{Dr_i})$ are sent.

  The doctor ensures the reliability of the HHS. Thus, the doctor uses his private key to verify the validity of HHS through RSA verification. When h_{Dr_i} matches with h'_{Dr_i}, the validity of Dr_i and HHS is ensured. Eventually, after completing the preceding procedures, the doctor and the HHS become trusted parties.
- **Attack resistance:** the proposed scheme is designed to resist well-known malicious attacks, such as MITM, replay, impersonation, DoS, and insider.
- **MITM and impersonation attacks:** This method is closely related to mutual authentication, thereby ensuring security even when attackers attempt to know one of the factors, such as the password or biometric. Obtaining both

authentication factors becomes difficult to the attackers; for example, the biometric is stored in a doctor's external device and the password is generated once at a time in addition to the anonymity for each independent login. Thus, the presented system confirmed the resistance of such attacks, as shown in Figs. 6 and 7 respectively.

- **Phishing attack:** an intruder (I_i) attempts to send a phish URL using an email to the patient (P_i) to obtain the sensitive information. When P_i clicks on the link and visits the I instead of the HHS server, P_i would be required encrypted credentials from the HHS. Thus, I_i has no option but to open a session with the actual HHS. Then, the HHS extracts the *URLI* to compare its parameters and sends OTP to P_i. Lastly, P_i inputs the OTP, and then the HHS verifies; if they match, then the *URLI* is safe; otherwise, the HHS decides that the *URLI* is an unauthorized server, and the phishing attack is prevented successfully.
- **Other types of attacks** include the security presented in our work according to r_i, the anonymity of username/password for the patient and the doctor, and the use of biometrics as an additional factor to increase the complexity of attacking process. Thus, the adversaries that perform negative attacks, failed to harm our system. Suppose that an adversary obtains some secret factors, he still cannot access the random number r, which is considered a prime factor in our security process. Therefore, our proposed system resists replay, DoS, and eavesdropping attacks because an adversary cannot access any exchanged parameter between the main system entities and the HHS.

V. Compassion of previous work

Table III compares the proposed scheme with related works depending on security metrics: P1 mutual authentication, P2 anonymity, P3 key agreement, P4 MITM attack, P5 impersonation attack, P6 replay attack, P7 DoS attack, P8 healthcare, P9 QR code, P10 signatures, P11 prescription, P12 data integrity, P13 forward/backward secrecy, and P14 phishing attack. Table IV shows the comparison of our scheme and the relevance based on taxonomy of the authentication scheme.

In addition, Table V provides a comparison of the computational cost between the most significant prior approaches and the present study, depending on the following scales:

T_h: Crypto hash function processing time.

T_F: Time of the fuzzy extractor operation's processing.

T_{Sg}: Processing time for signatures.

The estimated processing time for the essential functions are as follows: 0.0023 ms for T_h , 0.442 ms for T_F, and 0.085 ms for T_{Sg} [25, 26]. However, $T_{\oplus}$ and $T_{||}$ are neglected owing to their tiny time [27]. We suppose that the value (128 bit) of the communication cost of the login authentication phase is associated with the username, password, and crypto hash function. The value of the random number is (8 bit). Evidently, our work achieved the balance between the complexity and effective performance of the security.

TABLE V
Computational cost comparison

Protocol Scheme	Computation Cost	Total Cost (ms)
T. Wu et al. [24]	$18T_h + 4T_F$	1.81
Z. Xu et al. [28]	$10T_h$	0.023
Ryu and Kim [25]	$14T_h$	0.0322
Dhillon and Kalra [29]	$14T_h + 1T_{Sg}$	0.11
Proposed protocol	$5T_h + 2T_{Sg}$	0.16

In communication cost comparison, seven length variants were utilized as follows: (1) random numbers (128 bits), (2) identification (128 bits), (3) hash function (160 bits), (4) timestamp (32 bits), (5) symmetric key encryption (256 bits), (6) RSA digital signature (512 bits), and (7) Schnorr digital signature (512 bits). Table VI shows the communication costs of the relevant protocols.

TABLE VI
Communication costs of the relevant protocols

Protocol	Message length	Number of messages
T. Wu et al. [24]	3520 bits	5
Z. Xu et al. [28]	3136 bits	4
Ryu and Kim [25]	3872 bits	4
Dhillon and Kalra [29]	1248	2
Proposed protocol	1020	2

Our proposed system uses two exchanged messages during the communication process, including R_{Dr_i} data to HHS and R_{HHS} data to Dr_i and vice versa. As shown in Table 5, our total cost is 1020 bits. Accordingly, the proposed scheme is the lowest among the related works.

VI. CONCLUSIONS

In recent years, electronic health records have been widely promoted. Amidst these efforts, promoting safe EHR systems to maintain user and data protection is crucial. Therefore, this paper presented security countermeasures for healthcare systems. We have included several security measures, including user anonymization, mutual authentication, efficient smart login, and a secure data exchange channel to achieve a secure and robust login. One of the services provided is the safe release of the prescription prepared by doctors. The QR code was utilized during the transfer or request of the treatment from the pharmacy. Data integrity is achieved by ensuring the safety of the prescription when it reaches the pharmacist given that the prescription is signed by the doctor using RSA signature, and the treatment cannot be provided until the doctor's signature is verified. In addition, a higher level of security was obtained compared with other related works, and the proposed scheme balances the complexity of security and the communication cost.

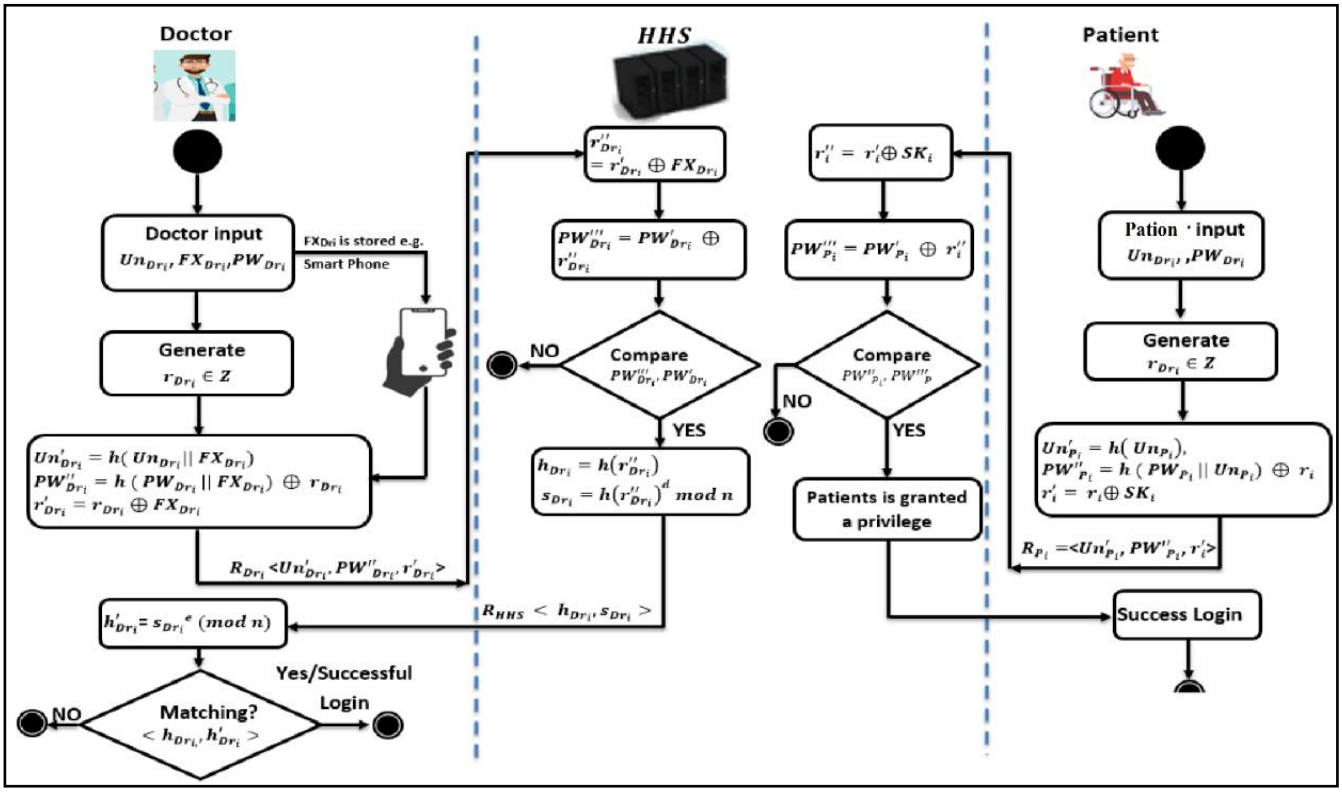

Fig. 3. Login and authentication phase

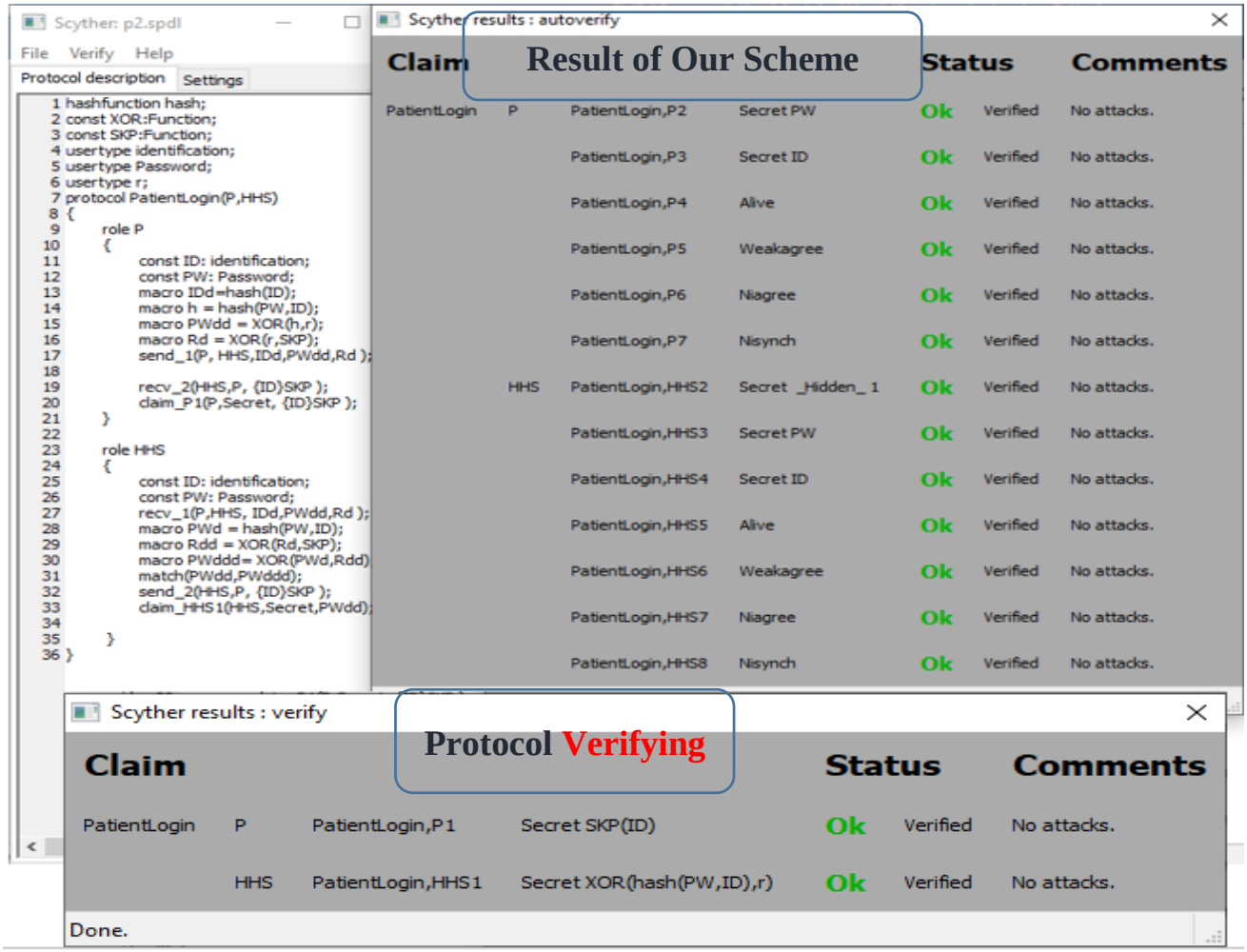

Fig. **6**. Patient's login protocol, verification, and automatic claim

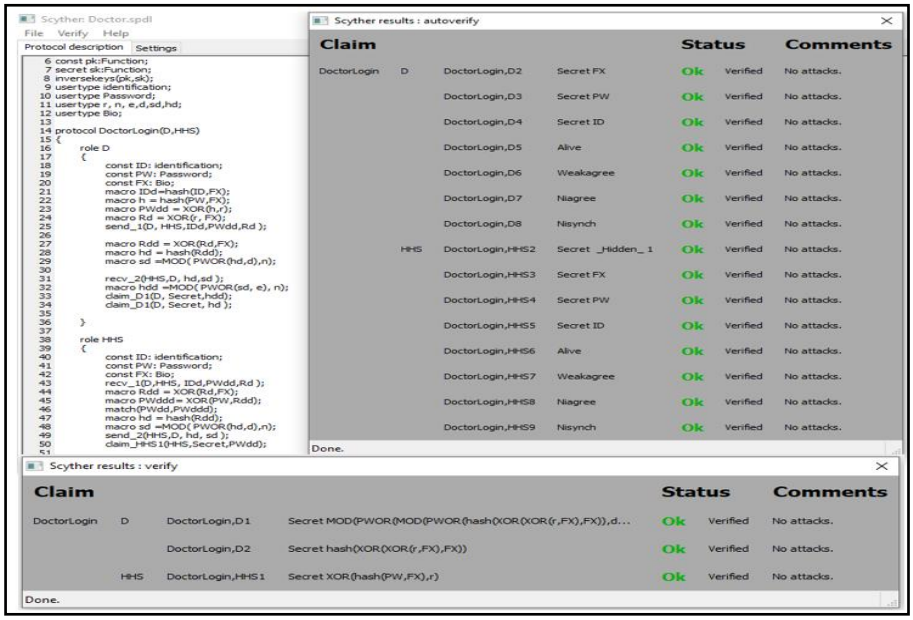

Fig. **7.** Doctor's login protocol

TABLE III
COMPARISON BASED ON SECURITY METRICS AND SCHEME'S FEATURES

Security Features	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
M. Bartłomiejczyk and M. Kurkowski [16]	☒	☒	☑	☑	☒	☑	☑	☒	☒	☒	☒	☒	☒	☒
Wu et al. [24]	☑	☑	☑	☑	☑	☑	☑	☒	☒	☒	☒	☑	☒	☒
Z. Xu et al. [28]	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Ryu and Kim [25]	☑	☑	☑	☑	☑	☑	☒	☑	☒	☒	☒	☒	☒	☒
Dhillon and Kalra [29]	☑	☑	☑	☑	☑	☑	☑	☑	☒	☒	☒	☑	☒	☒
Proposed Scheme	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

TABLE IV
COMPARISON BASED ON TAXONOMY OF AUTHENTICATION SCHEME

Reference	Year	Aim	Method	Cryptography Approach	Key-based	Security Evaluation
M. Bartłomiejczyk and M. Kurkowski [16]	2019	Multifactor authentication protocol in a mobile environment	MFA	OTP	Symmetric	Informal
T. Wu et al. [24]	2022	Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments	MFA	Hash function	Symmetric	Formal
Z. Xu et al. [28]	2019	A lightweight anonymous mutual authentication and key agreement scheme for WBAN	Two-FA	Hash function	Symmetric	Formal/ Informal
Ryu and Kim [25]	2021	Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications	Three-FA	Hash function	Symmetric	Formal/ Informal
Dhillon and Kalra [29]	2018	Multi-factor user authentication scheme for IoT-based healthcare services	Three-FA	Hash function	Symmetric	Formal/ Informal
Proposed Scheme	-	Secure Electronic Healthcare Record using Robust Authentication Scheme	MFA	Hash function/ RSA Signature	Symmetric	Formal/ Informal

REFERENCES

[1] A. Zriqat and M. Altamimi, "A Security Model For Preserving Privacy of Healthcare Information " *International Journal of Applied Engineering Research*, vol. 12, pp. pp. 14251-14258, 2017, Art. no. 24.

[2] J. Liang, C.-H. Tsou, and A. Poddar, "A novel system for extractive clinical note summarization using EHR data," In Proceedings of the *2nd clinical natural language processing workshop*, 2019, pp. 46-54.

[3] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-19, 2022.

[4] A. Singh, K. Chatterjee, "Trust based access control model for securing electronic healthcare system" *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4547-4565, 2019.

[5] M. Chen and T. Lin, "A Provable and Secure Patient Electronic Health Record Fair Exchange Scheme for Health Information Systems" *Applied Sciences*, vol. 11, no. 5, p. 2401, 2021.

[6] H. Chen, Z. Wu, T. Chen, Y. Huang, and C. Liu, "Security privacy and policy for cryptographic based electronic medical information system," *Sensors*, vol. 21, no. 3, p. 713, 2021

[7] N. A. Lal, S. Prasad, and M. J. Farik, "A review of authentication methods," vol. 5, pp. 246-249, 2016.

[8] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[9] K. Thomas et al., "Protecting accounts from credential stuffing with password breach alerting," In *28th August USENIX Security Symposium*, 2019, pp. 1556-1571.

[10] B. Chander and G. Kumaravelan, "An Improved 2-Factor Authentication Scheme for WSN Based on ECC," IETE Technical Review, pp. 1-12, 2022.

[11] A. Khan et al., "Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks," *IEEE Access*, vol. 10, pp. 31273-31288, 2022.

[12] D. Prabakaran and S. Ramachandran, "Multi-factor authentication for secured financial transactions in cloud environment," *CMC-Computers, Materials & Continua*, vol. 70, no. 1, pp. 1781-1798, 2022.

[13] A. Omotosho, O. Adegbola, O. Mikail, and J. Emuoyibofarhe, "A secure electronic prescription system using steganography with encryption key implementation," *arXiv preprint arXiv*:1502.01264, 2015.

[14] S. Jan, S. Ali, I. Abbasi, M. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, 2021.

[15] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 152-167, 2022.

[16] M. Bartłomiejczyk and M. Kurkowski, "Multifactor authentication protocol in a mobile environment," *IEEE Access*, vol. 7, pp. 157185-157199, 2019.

[17] T. Abayomi-Zannu, I. Odun-Ayo, and T. Barka, "A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication", *In Journal of Physics: Conference Series*, vol. 1378, p. 032104: IOP Publishing.

[18] H. Wahsheh and M. Al-Zahrani, "Secure and usable QR codes for healthcare systems: the case of covid-19 pandemic," in *2021 12th International Conference on Information and Communication Systems (ICICS)*. IEEE, Valencia, Spain, 2021. p. 324-329.

[19] A. Fauzi, N. Mohamed, H. Hashim, and M. Saleh, "Development of web-based smart security door using qr code system," in *2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*. *IEEE*, Shah Alam, Malaysia, 2020. p. 13-17.

[20] Y. Liu, Q. Zhong, L. Chang, Z. Xia, D. He, and C. Cheng, "A secure data backup scheme using multi-factor authentication," *IET Information security*, vol. 11, no. 5, pp. 250-255, 2017.

[21] A. Alhayajneh, A. Baccarini, G. Weiss, T. Hayajneh, and A. Farajidavar, "Biometric authentication and verification for medical cyber physical systems", *Electronics*, vol. 7, no. 12, p. 436, 2018.

[22] H. Yang, V. Oleshchuk, and A. Prinz, "Verifying Group Authentication Protocols by Scyther," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 7, no. 2, pp. 3-19, 2016.

[23] H. Yang, A. Prinz, and V. Oleshchuk, "Formal analysis and model checking of a group authentication protocol by Scyther," in *2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*. IEEE, Heraklion, Greece, 2016. p. 553-557.

[24] T. Wu, Q. Meng, S. Kumari, and P. Zhang, "Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments," *Sensors*, vol. 22, no. 10, p. 3858, 2022.

[25] H. Ryu and H. Kim, "Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications," in *Healthcare*, 2021, vol. 9, no. 9, p. 1114: MDPI.

[26] H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE communications surveys & tutorials*, vol. 16, no. 2, pp. 1005-1023, 2013.

[27] M. Ibrahim, S. Kumari, A. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Computer methods and programs in biomedicine*, vol. 135, pp. 37-50, 2016.

[28] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurrency and computation: Practice and experience*, vol. 31, no. 14, p. e5295, 2019.

[29] P. Dhillon and S. Kalra, "Multi-factor user authentication scheme for IoT-based healthcare services," *Journal of Reliable Intelligent Environments*, vol. 4, pp. 141-160, 2018.